UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MASSACHUSETTS

IN RE: MOVEIT CUSTOMER DATA SECURITY BREACH LITIGATION This Document Relates To: KATHARINE UHRICH, individually and on behalf of all others similarly situated, PLAINTIFF, v. TEACHERS INSURANCE AND ANNUITY ASSOCIATION OF AMERICA, PENSION BENEFIT INFORMATION, LLC, and PROGRESS SOFTWARE CORPORATION, DEFENDANTS.	MDL NO. 1:23-md-03083-ADB-PGL **AMENDED CLASS ACTION COMPLAINT** CIVIL ACTION NO. 1:23-cv-12785

Plaintiff Katharine Uhrich, individually and on behalf of all others similarly situated, brings this Class Action Complaint against Defendants Teachers Insurance and Annuity Association of America ("TIAA"), Pension Benefit Information, LLC ("PBI"), and Progress Software Corporation ("PSC") (collectively, "Defendants"), to seek redress for the Defendants' conduct leading up to, surrounding, and following a data vulnerability and breach incident that exposed the personal information of millions of people. Plaintiff alleges as follows upon personal knowledge as to herself and her own acts and experiences, and as to all other matters, upon information and belief, including an investigation conducted by her attorneys.

NATURE OF CASE

1. Plaintiff incorporates the allegations contained in Plaintiffs' Omnibus Set of Additional Pleading Facts (ECF No. 908) in its entirety.

2. TIAA is a New York based insurance and financial service company that operates in all 50 states, including the state of Illinois.

3. PBI acts as a pension plan "sponsor, administrator, or record keeper" "for thousands of organizations" and pension plans, including TIAA. PBI uses PSC's MOVEit service in the regular course of its business.

4. Defendants failed to safeguard the confidential personal identifying information of the Plaintiff and numerous other individuals ("Class Members" or collectively as the "Class"). This class action is brought on behalf of Class Members whose personally identifiable information ("PII", or "Private Information") was accessed through the Defendants' systems without their permission or knowledge.

5. As explained in detail herein, an unauthorized third party accessed Defendants' MOVEit Transfer servers and accessed and removed PII from the server as early as May 27, 2023 (the "Data Breach").

6. Defendants' failures to implement or maintain adequate data security measures for PII directly and proximately caused injuries to Plaintiff and the Class.

7. Defendants failed to take reasonable steps to employ adequate security measures or to properly protect sensitive PII despite well-publicized data breaches at numerous businesses and financial institutions in recent years.

8. Despite numerous and high-profile data breaches, Defendants failed to implement basic security measures to prevent unauthorized access to this information.

9. Citizens from across Illinois and the United States have suffered real and imminent harm as a direct consequence of the Defendants' conduct, which included: (a) refusing to take adequate and reasonable measures to ensure their data systems, as well as the data stored therein,

were protected; (b) refusing to take available steps to prevent the Breach from happening; (c) failing to disclose to consumers the material facts that they did not have adequate computer systems and security practices to safeguard Private Information; and (d) failing to provide timely and adequate notice of the Data Breach.

10. The Data Breach was the inevitable result of Defendants' inadequate data security measures and approach to data security. Despite the well-publicized and ever-growing threat of security breaches, and even though data breaches were and are occurring across numerous industries, Defendants failed to ensure that they maintained adequate data security measures causing the Private Information of Plaintiff and Class Members to be stolen.

11. As a direct and proximate consequence of Defendants' negligence, a massive amount of customer information was stolen from Defendants. Victims of the Data Breach have had their Private Information compromised, had their privacy rights violated, been exposed to the increased risk of fraud and identify theft, lost control over their personal and financial information, and otherwise been injured.

12. Plaintiff brings this class action lawsuit on behalf of those similarly situated to address Defendants' inadequate safeguarding of Class Members' Private Information that they collected and maintained, and for failing to provide timely and adequate notice to Plaintiff and other Class Members that their information had been subject to the unauthorized access of an unknown third party.

JURISDICTION AND VENUE

13. This case was originally filed in the United States District Court for the Northern District of Illinois. This action has been transferred to this Court for coordinated or consolidated

pretrial proceedings pursuant to 28 U.S.C. § 1407 and Rule 7.1 of the Rules of Procedure of the United States Judicial Panel on Multidistrict Litigation.

14. This Court has jurisdiction over this case pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d), because Plaintiff and at least one member of the Class, as defined below, is a citizen of a different state than Defendants, there are more than 100 putative class members, and the aggregate amount in controversy exceeds $5,000,000, exclusive of interest and costs.

15. This Court has supplemental jurisdiction over Plaintiff's state law claims under 28 U.S.C. § 1367.

16. The United States District Court for the Northern District of Illinois has personal jurisdiction over Defendants because Plaintiff contracted with TIAA from that District, resides in and was harmed in that District. Defendants have sufficient contacts in Illinois, as they conduct a significant amount of business in the state of Illinois.

17. Venue is proper in the United States District Court for the Northern District of Illinois pursuant to 28 U.S.C. § 1391 because a substantial part of the events, omissions, and acts giving rise to the claim occurred in that District. Moreover, Plaintiff resides in that District.

PARTIES

18. Plaintiff Katharine Uhrich ("Plaintiff" or "Mrs. Uhrich") was a resident and citizen of Illinois during all times relevant.

19. Plaintiff used TIAA as a retirement service provider when working for her former employer. Plaintiff provided Defendants with her personal information in order to create and maintain an account with TIAA, and trusted Defendants to maintain her personal information in a safe and secure manner.

20. Plaintiff became aware that her PII had been involved in the Data Breach when she received a letter from PBI dated July 25, 2023. (Exhibit A, Data Breach Letter).

21. TIAA is a corporation organized under the laws of New York, with its principal place of business located in New York.

22. TIAA is a Vendor Contracting Entity of PBI. (*See* Plfs.' Omnibus Set of Addtl. Pleading Facts, App. A.)

23. PBI is a for-profit Delaware corporation with its principal place of business at 333 S 7th Street, Suite 2400, Minneapolis, MN 55402. PBI uses PSC's MOVEit service in the regular course of its business acting as a pension plan "sponsor, administrator, or record keeper" "for thousands of organizations" and pension plans.[1]

24. PBI is a PSC Vendor. (*See* Plfs.' Omnibus Set of Addtl. Pleading Facts, App. A.)

25. PSC is a Delaware corporation and maintains its headquarters and principal place of business at 15 Wayside Road, 4th Floor, Burlington, Massachusetts 01803. PSC offers the service MOVEit, which experienced the Data Breach underlying Plaintiff's claims.

FACTUAL ALLEGATIONS

A. The Data Breach

26. Defendants obtained significant PII from consumers throughout the United States, including that of Plaintiff and the Class Members, as a result of their business operations.

27. On or around July 14, 2023, TIAA announced that it had previously, on or about May 31, 2023, suffered a data breach that impacted millions of individuals.

28. Plaintiff's and Class Members' sensitive PII, which was entrusted to Defendants, was compromised, unlawfully accessed, and stolen due to the Data Breach.

[1] https://www.pbinfo.com/ (last visited August 1, 2023).

29. On information and belief, at minimum, significant PII was included in the Data Breach:

A. Name;

B. Social Security number;

C. Gender;

D. Date of birth; and

E. Address.

30. As a result of Defendants' actions and/or inactions, Plaintiff and the Class Members were harmed and must now take remedial steps to protect themselves from future loss. Indeed, Plaintiff and all Class Members are currently at a very high risk of misuse of their Private Information in the coming months and years, including but not limited to unauthorized account access including on third-party services and identity theft through use of personal information to open up accounts.

31. As a result of Defendants' failure to properly and timely notify consumers of the full extent of the Data Breach, members of the Class have not had the opportunity to fully protect themselves and take any specific precautions.

32. The unauthorized access occurred because third parties were able to access Plaintiff's and the Class's PII because Defendants failed to take reasonable measures to protect the Private Information they collected and stored. Among other things, Defendants failed to implement data security measures designed to prevent this attack, despite repeated industry wide warnings about the risk of cyberattacks and the highly publicized occurrence of many similar attacks in the recent past.

33. As a result of Defendants' failure to properly secure Plaintiff's and the Class Members' PII, Plaintiff's and the Class Members' privacy has been invaded.

34. Moreover, all of this Private Information is likely for sale to criminals on the dark web, meaning that unauthorized parties have likely accessed and viewed Plaintiff's and Class Members' PII.

B. Data Breaches and Industry Standards of Protection of PII

35. Identity theft, which costs Americans billions of dollars a year, occurs when an individual's PII is used without his or her permission to commit fraud or other crimes. Victims of identity theft typically lose hundreds of hours dealing with the crime, and they typically lose hundreds of dollars.

36. According to the Federal Trade Commission ("FTC"):

> Identity theft is serious. While some identity theft victims can resolve their problems quickly, others spend hundreds of dollars and many days repairing damage to their good name and credit record. Some consumers victimized by identity theft may lose out on job opportunities, or be denied loans for education, housing or cars because of negative information on their credit reports. In rare cases, they may even be arrested for crimes they did not commit.

37. The United States Government Accountability Office ("GAO") has stated that identity thieves can use identifying data to open financial accounts and incur charges and credit in a person's name. As the GAO has stated, this type of identity theft is the most damaging because it may take some time for the victim to become aware of the theft and can cause significant harm to the victim's credit rating. Like the FTC, the GAO explained that victims of identity theft face "substantial costs and inconvenience repairing damage to their credit records," as well the damage to their "good name."

38. Industry Standards highlight several basic cybersecurity safeguards that can be implemented to improve cyber resilience that require a relatively small financial investment yet can have a major impact on an organization's cybersecurity posture including: (a) the proper encryption of Private Information; (b) educating and training employees on how to protect Private Information; and (c) correcting the configuration of software and network devices.

39. Identity theft crimes often encompass more than just immediate financial loss. Identity thieves often hold onto stolen personal and financial information for several years before using and/or selling the information to other identity thieves.

40. Accordingly, federal and state legislatures have passed laws to ensure companies protect the security of sensitive personally identifying confidential information, such as that wrongfully disclosed in the Data Breach.

41. The FTC has issued a publication entitled "Protecting Personal Information: A Guide for Business" ("FTC Report"). The FTC Report provides guidelines for businesses on how to develop a "sound data security plan" to protect against crimes of identity theft. To protect the personal sensitive information in their files, the FTC Report instructs businesses to follow, among other things, the following guidelines:

A. Know what personal information you have in your files and on your computers;

B. Keep only what you need for your business;

C. Protect the information that you keep;

D. Properly dispose of what you no longer need;

E. Control access to sensitive information by requiring that employees use "strong" passwords; tech security experts believe the longer the password, the better; and

F. Implement information disposal practices reasonable and appropriate to prevent an unauthorized access to personally identifying information.

42. The FTC Report also instructs companies that outsource any business functions to proactively investigate the data security practices of the outsourced company and examine their standards.

43. The Federal Trade Commission ("FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

C. Defendants Failed to Prevent the Data Breach, Putting Plaintiff and Class Members at Risk

44. Upon information and belief, Defendants have policies and procedures in place regarding the safeguarding of confidential information they are entrusted with, and Defendants failed to comply with those policies.

45. Upon information and belief, in the course of collecting PII from consumers, including Plaintiff, Defendants promised to provide confidentiality and adequate security for consumer data through their applicable privacy policies and through other disclosures in compliance with statutory privacy requirements.

46. Indeed, TIAA's Privacy Notice provides that: "TIAA protects the personal information you provide against unauthorized access, disclosure, alteration, destruction, loss, or misuse. Your personal information is protected by physical, electronic, and procedural safeguards in accordance with federal and state standards. These safeguards include appropriate procedures for access and use of electronic data, provisions for the secure transmission of sensitive personal

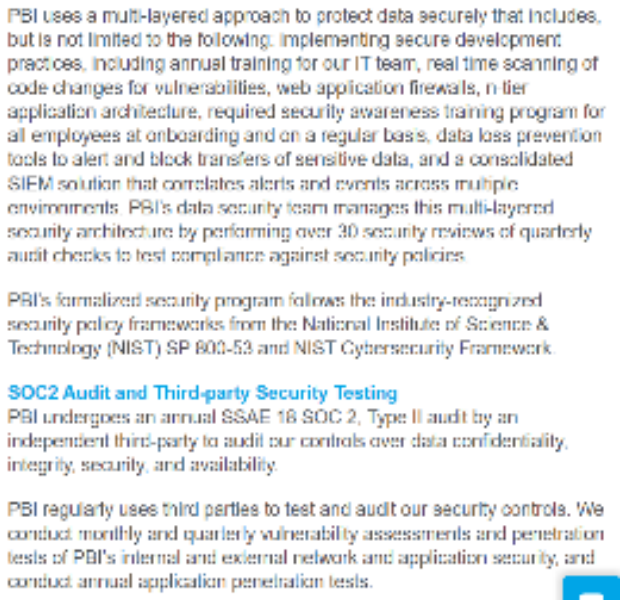
information on our website, and telephone system authentication procedures. Additionally, we limit access to your personal information to those TIAA employees and agents who need access in order to offer and provide products or services to you. We also require our service providers to protect your personal information by utilizing the privacy and security safeguards required by law."[2]

47. PBI is a pension plan "sponsor, administrator, or record keeper" "for thousands of organizations" and pension plans, and one of the many companies that uses PSC's MOVEit service to transfer large amounts of data in the ordinary course of its business and the service it provides to pension plans and other organizations.[3]

48. According to the Notice Letter received by Plaintiff, PBI provides audit and address research services for TIAA.

49. PBI's website also promises consumers that it has robust systems and processes in place to protect and secure their sensitive information:

[2] https://www.tiaa.org/public/support/privacy/privacy-notice (last visited Sept. 11, 2023).
[3] https://www.pbinfo.com/ (last visited August 1, 2023).



50. PBI's website also tells consumers that it has systems and process in place to ensure the privacy of their sensitive information obtained over the internet and to prevent identity theft:

> **9. ONLINE PRIVACY**
>
> PBI strives to protect the privacy of personally identifiable information obtained over the Internet and strives to apply the Principles and evolving standards to the online environment.
>
> **10. IDENTITY THEFT**
>
> PBI strives to prevent the acquisition of information from our products and services for improper purposes, such as identity theft. PBI believes in the importance of notifying individuals who may have had their sensitive personally identifiable information acquired by an unauthorized individual, as appropriate.

51. Furthermore, PBI acknowledges that it has a duty to safeguard Plaintiff's and Class Members' sensitive PII because, *inter alia*, PBI's website tells consumers that it has systems in place to protect consumers' sensitive information, and routinely audits those systems to ensure

they are compliant with federal regulations and other legislation—as well as industry standards and practices— governing data privacy:

> **8. ACCOUNTABILITY**
>
> PBI supports accountability of information industry standards and practices, responsible and effective federal regulation of the data industry, and legislation governing the practices of all data providers. PBI also supports industry oversight and active engagement with the privacy community. PBI believes that strong privacy and information security protections are vital for an effective and trusted data industry.
>
> **11. COMPLIANCE**
>
> PBI will obtain assessments from an independent auditor, who uses procedures and standards generally accepted in the profession to assess PBI's controls relevant to security, availability, and confidentiality, as appropriate.

52. Discovery will show that through its provision of the foregoing services, PBI obtains possession of customers'—including Plaintiff's and Class Members'—highly sensitive PII. Thus, in the regular course of its business, PBI collects and/or maintains the PII of consumers such as Plaintiff and Class Members. PBI stores this information digitally in the regular course of business.

53. As evidenced by, *inter alia*, their receipt of the notice informing them that their PII were compromised in the Data Breach, Plaintiff's and Class Members' PII was transferred using PSC's MOVEit service and/or they otherwise entrusted to Defendants their PII, from which Defendants profited.

54. Yet, contrary to their representations—by virtue of Defendants' admissions that they experienced the Data Breach—Defendants did not have adequate measures in place to protect and maintain sensitive PII entrusted to them. Instead, Defendants' websites wholly fail to disclose the truth: that Defendants lack sufficient processes to protect the PII that is entrusted to them.

55. In the course of their relationship, consumers, including Plaintiff and Class Members, provided Defendants, directly or indirectly, with at least the following PII:

- names;
- gender;
- dates of birth;
- Social Security numbers; and
- addresses.

56. In the course of their ordinary business operations, Defendants are entrusted with safeguarding the sensitive PII of TIAA members.

57. Defendants negligently failed to comply with industry standards or even implement rudimentary security practices, resulting in Plaintiff's and the Class's PII being substantially less safe than had this information been entrusted with other similar companies.

58. Defendants were aware of the likelihood and repercussions of cyber security threats, including data breaches, having doubtlessly observed numerous other well-publicized data breaches involving major corporations over the last decade- as well as the numerous other similar data breaches preceding those major breaches.

59. In addition to Defendants' failure to prevent the Data Breach, they also failed to timely detect the Data Breach and realize this Private Information remained publicly accessible and unencrypted for a substantial amount of time.

60. Hackers, cyber-criminals, and other nefarious actors, therefore, had sufficient time to collect this Private Information unabated. During this time, Defendants failed to recognize the failure to protect this Private Information. If Defendants had quickly detected the Data Breach, this likely would have significantly reduced the consequences of the Data Breach. Instead, Defendants' delay in detecting the Data Breach contributed to the scale of the Data Breach and the resulting damages.

61. The Data Breach occurred because Defendants failed to implement adequate data security measures to protect their databases and computer systems from the potential dangers of a data breach and failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the Private Information compromised in the Data Breach.

62. The Data Breach was caused and enabled by Defendants' knowing violation of their obligations to abide by best practices and industry standards in protecting Private Information.

D. The Data Breach Caused Current and Future Harm

63. As a direct and proximate result of Defendants' wrongful disclosure, criminals now have Plaintiff's and the Class Members' Private Information.

64. Defendants' wrongful actions and inactions here directly and proximately caused the public disclosure of Plaintiff's and Class Members' personal identifying information without their knowledge, authorization and/or consent. As a further direct and proximate result of Defendants' wrongful actions and/or inactions, Plaintiff and Class Members have suffered, and will continue to suffer, damages including, without limitation, expenses for credit monitoring and identity theft insurance, out-of-pocket expenses, anxiety, emotional distress, loss of privacy, and other economic and non-economic harm.

65. As a further result of the Data Breach, Plaintiff and Class Members have been exposed to a substantial and present risk of fraud and identity theft. Plaintiff and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft.

66. By way of example, Plaintiff has experienced a substantial increase in spam and phishing calls since the Data Breach.

67. Identity thieves can use personal information, such as that of Plaintiff and the other Class Members, which Defendants failed to keep secure, to perpetrate a variety of crimes that harm

victims. Even basic personal information, combined with other contact information, is very valuable to hackers and identity thieves as it allows them to access users' other accounts. Thus, even if some information was not involved in the Data Breach, the unauthorized parties could use Plaintiff's and Class Members' Private Information to access other information, including, but not limited to email accounts, government services accounts, e-commerce accounts, payment card information, and financial accounts, to engage in the fraudulent activity identified by Plaintiff.

68. Defendants were at all times fully aware of their obligations to protect the Private Information of Plaintiff and Class Members. Plaintiff and Class Members would not have entrusted their Private Information to Defendants had they known that Defendants would fail to maintain adequate data security. Defendants were also aware of the significant repercussions that would result from their failure to do so.

69. Reimbursing a consumer for a financial loss due to fraud does not make that individual whole again. Identity theft victims must spend numerous hours and their own money repairing the impact to their credit.

70. Thus, Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights.

71. Plaintiff has already had to expend her personal time contacting the credit bureaus to freeze her credit files, and has had to increase her time spent monitoring her accounts for suspicious activity.

72. Defendants' wrongful actions and inaction directly and proximately caused the theft and dissemination into the public domain of Plaintiff, the other Class Members' Private Information, causing them to suffer, and continue to suffer, economic damages and other actual harm for which they are entitled to compensation, including but not limited to:

a. Theft of their Private Information and financial information;

b. Costs for credit monitoring services; unauthorized charges on their debit and credit card accounts;

c. Unauthorized charges on their debit and credit cards;

d. Injury flowing from potential fraud and identity theft posed by their Private Information being placed in the hands of criminals and already misused via the sale of Plaintiff and Class Members' Private Information on the black market and dark web;

e. Losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach;

f. Losses in the form of deprivation of the value of their Private Information;

g. The untimely and inadequate notification of the Data Breach;

h. The improper disclosure of their Private Information;

i. Loss of privacy;

j. Loss of use of, and access to, their account funds and costs associated with the inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit including adverse credit notations; and,

k. The loss of productivity and value of their time spent to address, attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach, including finding fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services.

73. Additionally, even with credit monitoring, the damages of a Data Breach will last much longer since this Private Information cannot be completely removed from the possession of cybercriminals. In fact, it will likely continue to circulate on the dark web and be sold or traded to other hackers and cybercriminals or identity thieves who will use it to continue to perpetuate fraud against the Class Members.

74. Although the Private Information of Plaintiff and the Class Members has been stolen, Defendants continue to hold Private Information of the affected individuals, including Plaintiff and the Class Members.

75. Particularly, because Defendants have demonstrated an inability to prevent a data breach or stop it from continuing even after being detected and informed of the impermissible dissemination—Plaintiff, the other Class Members, have an undeniable interest in ensuring their Private Information is secure, remains secure, is properly and promptly destroyed, and is not subject to further disclosure and theft.

76. Accordingly, Plaintiff on behalf of herself and the Class, bring this action against Defendants seeking redress for their unlawful conduct.

CLASS ALLEGATIONS

77. Plaintiff brings this nationwide class action on behalf of herself and on behalf of others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

78. Specifically, Plaintiff proposes the following classes (collectively, the "Class"):

(1) PSC Nationwide Class: All persons whose Private Information was compromised in the MOVEit data breach.

(a) PSC Illinois Class: All residents of Illinois whose Private Information was compromised in the MOVEit data breach.

(2) PBI Nationwide Class: All persons whose Private Information was compromised on PBI's platform and/or systems in the MOVEit data breach.

(a) PBI Illinois Class: All residents of Illinois whose Private Information was compromised on PBI's platform and/or systems in the MOVEit data breach.

(3) TIAA Nationwide Class: All persons whose Private Information was compromised in the MOVEit data breach where such Private Information was obtained from or hosted by TIAA.

(a) TIAA Illinois Class: All residents of Illinois whose Private Information was compromised in the MOVEit data breach where such Private Information was obtained from or hosted by TIAA.

The foregoing state-specific classes are collectively referred to as the "State Classes" and the foregoing nationwide classes are collectively referred to as the "Nationwide Classes."

79. Excluded from the Class are Defendants, their parents, subsidiaries, affiliates, officers, and directors, all persons who make a timely election to be excluded from the Class, the judge to whom this case is assigned and any immediate family members thereof, and the attorneys who enter their appearance in this action.

80. Plaintiff may alter the class definitions to conform to developments in the case and discovery.

81. The proposed Class meets all requirements under Fed. R. Civ. P. 23.

82. **Numerosity:** Upon information and belief, the Class is so numerous that joinder of all individuals would be impracticable. The exact number of members of the Class is presently unknown and can only be ascertained through discovery because that information is exclusively in the possession of Defendants. However, it is reasonable to infer that more than 40 individuals in each of the Classes were impacted by the Data Breach at issue. Members of the Class can be easily identified through Defendants' records. Class Members may be notified of the pendency of

this action by recognized, Court-approved notice dissemination methods, which may include U.S. mail, electronic mail, Internet postings, and/or published notice.

83. **Commonality:** This action involves common questions of law and fact, which predominate over any questions affecting individual members of the Class, including, without limitation:

A. Whether Defendants negligently failed to maintain and execute reasonable procedures designed to prevent unauthorized access to Plaintiff's and Class Members' PII;

B. Whether Defendants were negligent in storing and failing to adequately safeguard Plaintiff's and Class Members' PII;

C. Whether Defendants owed a duty to Plaintiff and Class Members to exercise reasonable care in protecting and securing their PII;

D. Whether Defendants breached their duties to exercise reasonable care in failing to protect and secure Plaintiff's and Class Members' PII;

E. Whether by disclosing Plaintiff's and Class Members' PII without authorization, Defendants invaded Plaintiff's and Class Members' privacy;

F. Whether Plaintiff and Class Members sustained damages as a result of Defendants' failure to secure and protect their PII.

84. **Typicality**: Plaintiff's claims are typical of the claims of the Class Members, as they are all based on the same factual and legal theories. Plaintiff and all Class Members sustained damages arising out of and caused by the Defendants' common course of conduct in violation of law.

85. **Adequacy of Representation:** Plaintiff is an adequate representative of the Class because her interests do not conflict with the interests of the members of the Class she seeks to represent, and she intends to prosecute this action vigorously. Plaintiff has retained counsel competent and experienced in consumer class actions and complex litigation. The interests of the Class will be fairly and adequately protected by Plaintiff and her counsel and Plaintiff's claims are typical of the claims of the Class Members.

86. **Superiority:** A class action in this case would be appropriate and superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages or other financial detriment suffered by Plaintiff and members of the Class are relatively small compared to the burden and expense that would be required to individually litigate their claims against the Defendants, so it would be impracticable for members of the Class to individually seek redress for the Defendants' wrongful conduct. Individualized litigation creates a potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the judicial system. By contrast, the class action device presents far fewer management difficulties, and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

87. **Ascertainability:** The Class Members are easily ascertainable from the Defendants' records and it would not be difficult to obtain this specific information in discovery.

88. Defendants have acted or failed to act on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class-wide basis.

89. Class certification, therefore, is appropriate pursuant to Rule 23 because the above common questions of law or fact predominate over any questions affecting individual Class Members, and a class action is superior to other available methods for the fair and efficient adjudication of this controversy.

COUNT I - NEGLIGENCE

(*On Behalf of Plaintiff and the Nationwide Classes, and the State Classes in the Alternative, Against All Defendants*)

90. Plaintiff re-alleges the preceding paragraphs as if set forth fully in this Count.

91. Defendants obtained sensitive Private Information about Plaintiff and Class Members.

92. Upon Defendants' accepting and storing the Private Information of Plaintiff and the Class in their computer systems and on their networks, Defendants undertook and owed a duty to Plaintiff and the Class to exercise reasonable care to secure and safeguard that information and to use commercially reasonable methods to do so. Defendants knew that the Private Information was private and confidential and should be protected as private and confidential.

93. Defendants owed a duty of care not to subject Plaintiff's and the Class Members' Private Information to an unreasonable risk of exposure because Plaintiff and the Class were foreseeable and probable victims of any inadequate security practices.

94. Defendants owed a duty to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting their PII in their possession from being compromised, lost, stolen, accessed or misused by unauthorized persons. More specifically, this duty included, among other things: (a) designing, maintaining, and testing their security systems, as well as those of any contractors, to ensure that Plaintiff's and Class Members'

PII in Defendants' possession was adequately secured and protected; (b) implementing processes that would detect a breach of their security systems in a timely manner; (c) timely acting upon warnings and alerts, including those generated by their own security systems, regarding intrusions to their networks; and (d) maintaining data security measures consistent with industry standards.

95. It was reasonably foreseeable that Defendants' failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class Members' Private Information would result in an unauthorized third-party gaining access to such information without Plaintiff's or Class Members' knowledge or consent.

96. Defendants knew, or should have known, of the risks inherent in collecting, storing, and sharing Private Information amongst themselves and the importance of adequate security. Defendants knew of should have known about numerous well-publicized data breaches within the industry.

97. Defendants' duty to use reasonable security measures also arose as a result of the special relationship that existed between Defendants, on the one hand, and Plaintiff and Class Members, on the other hand.

98. The special relationship arose because Plaintiff and Class Members entrusted Defendants with their PII as part of the use of the Defendants' products and services. Defendants alone could have ensured that their security systems and data storage architecture were sufficient to prevent or minimize the Data Breach.

99. Defendants' duty also arose under Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect PII by companies such as Defendants. Various FTC publications and data

security breach orders further form the basis of Defendants' duty. In addition, individual states have enacted statutes based upon the FTC Act that also created a duty.

100. Defendants also had a duty to safeguard the PII of Plaintiff and Class Members and to promptly notify them of a breach because of state laws and statutes that require Defendants to reasonably safeguard sensitive PII, as detailed herein.

101. Defendants breached the duties they owed to Plaintiff and Class Members described above and thus were negligent.

102. Defendants breached these duties by, among other things, failing to: (a) exercise reasonable care and implement adequate security systems, protocols and practices sufficient to protect the PII of Plaintiff and Class Members; (b) immediately detect the Breach while it was ongoing; (c) maintain security systems consistent with industry standards during the period of the Data Breach; (d) comply with regulations protecting the PII at issue during the period of the Data Breach; and (e) disclose in a timely and adequate manner that Plaintiff's and the Class Members' PII in Defendants' possession had been or was reasonably believed to have been, stolen or compromised.

103. But for Defendants' wrongful and negligent breach of the duties owed to Plaintiff and Class Members, their PII would not have been compromised.

104. Defendants' failure to take proper security measures to protect the sensitive PII of Plaintiff and Class Members created conditions conducive to a foreseeable, intentional act, namely the unauthorized access of Plaintiff's and Class Members' PII.

105. Plaintiff and Class Members were foreseeable victims of Defendants' inadequate data security practices, and it was also foreseeable that Defendants' failure to provide timely and

adequate notice of the Data Breach would result in injury to Plaintiff and Class Members as described in this Complaint.

106. Plaintiff and the Class Members were (and continue to be) damaged as a direct and proximate result of Defendants' failure to secure and protect their Private Information.

107. Defendants' wrongful actions and/or inactions (as described above) constituted, and continue to constitute, negligence at common law.

COUNT II – BREACH OF CONFIDENCE

(*On Behalf of Plaintiff and the Nationwide Classes, and the State Classes in the Alternative, Against All Defendants*)

108. Plaintiff re-alleges the preceding paragraphs as if set forth fully in this Count.

109. Plaintiff and Class Members maintained a confidential relationship with Defendants whereby Defendants undertook a duty not to disclose to unauthorized parties the Plaintiff's and Class Members' PII to unauthorized third parties. Such PII was confidential and novel, highly personal and sensitive, and not generally known.

110. Defendants knew Plaintiff's and Class Members' PII was being disclosed in confidence and understood the confidence was to be maintained, including by expressly and implicitly agreeing to protect the confidentiality and security of the PII they collected, stored, and maintained.

111. As a result of the Data Breach, there was an unauthorized disclosure of Plaintiff's and Class Members' PII in violation of this understanding. The unauthorized disclosure occurred because Defendants failed to implement and maintain reasonable safeguards to protect the PII in their possession and failed to comply with industry-standard data security practices.

112. Plaintiff and Class Members were harmed by way of a disclosure of their confidential information to an unauthorized third party to which they did not consent.

113. But for Defendants' disclosure of Plaintiff's and Class Members' PII in violation of the parties' understanding of confidence, their PII would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties.

114. The Data Breach was the direct and legal cause of the theft of Plaintiff's and Class Members' PII, as well as the resulting damages.

115. The injury and harm Plaintiff and Class Members suffered was the reasonably foreseeable result of Defendants' unauthorized disclosure of Plaintiff's and Class Members' PII.

116. Defendants knew their computer systems and technologies for accepting, securing, and storing Plaintiff's and Class Members' PII had serious security vulnerabilities because they failed to observe standard security practices or correct known security vulnerabilities.

117. As a direct and proximate result of Defendants' violations, Plaintiff and the Class have suffered and continue to suffer injury.

COUNT III - INVASION OF PRIVACY BY PUBLIC DISCLOSURE OF PRIVATE FACTS AND INTRUSION UPON SECLUSION

(*On Behalf of Plaintiff and the Nationwide Classes, and the State Classes in the Alternative, Against All Defendants*)

118. Plaintiff re-alleges the preceding paragraphs as if set forth fully in this Count.

119. Plaintiff's and Class Members' Private Information is and always has been private and confidential.

120. Dissemination of Plaintiff's and Class Members' Private Information is not of a legitimate public concern; publication to third parties of their Private Information would be, is and will continue to be, offensive to Plaintiff, Class Members, and other reasonable people.

121. By failing to keep Plaintiff's and Class Members' PII secure, and disclosing PII to unauthorized parties for unauthorized use, Defendants unlawfully invaded Plaintiff's and Class Members' privacy right to seclusion by, inter alia:

A. Intruding into their private affairs in a manner that would be highly offensive to a reasonable person;

B. Invading their privacy by improperly using their PII properly obtained for specific purpose for another purpose, or disclosing it to unauthorized persons;

C. Failing to adequately secure their PII from disclosure to unauthorized persons; and

D. Enabling the disclosure of their PII without consent.

122. Defendants' wrongful actions and/or inactions (as described above) constituted, and continue to constitute, an invasion of Plaintiff's and Class Members' privacy by publicly disclosing their Private Information.

123. Defendants' intrusions were substantial and would be highly offensive to a reasonable person, constituting an egregious breach of social norms.

124. Plaintiff and the Class Members were (and continue to be) damaged as a direct and proximate result of Defendants' invasion of their privacy by publicly disclosing their Private Information, for which they suffered loss and are entitled to compensation.

125. As a direct and proximate result of Defendants' violations, Plaintiff and the Class have suffered and continue to suffer injury.

COUNT IV - BREACH OF CONTRACT

(*On Behalf of Plaintiff and the Nationwide Classes, and the State Classes in the Alternative, Against All Defendants*)

126. Plaintiff re-alleges the preceding paragraphs as if set forth fully in this Count.

127. Plaintiff and other Class Members entered into valid and enforceable express contracts with Defendants under which Plaintiff and other Class Members agreed to provide their Private Information to Defendants, and Defendants impliedly, if not explicitly, agreed to protect Plaintiff's and Class Members' Private Information.

128. To the extent Defendants' obligation to protect Plaintiff's and other Class Members' Private Information was not explicit in those express contracts, the express contracts included implied terms requiring Defendants to implement data security adequate to safeguard and protect the confidentiality of Plaintiff's and other Class Members' Private Information, including in accordance with federal, state and local laws, regulations, and industry standards. Neither Plaintiff nor any Class Member would have entered into these contracts with Defendants without the understanding that Plaintiff's and other Class Members' Private Information would be safeguarded and protected; stated otherwise, data security was an essential implied term of the parties' express contracts.

129. A meeting of the minds occurred, as Plaintiff and Class Members agreed, among other things, to provide their Private Information in exchange for Defendants' agreement to protect the confidentiality of that Private Information.

130. The protection of Plaintiff's and Class Members' Private Information was a material aspect of Plaintiff's and Class Members' contracts with Defendants.

131. Plaintiff and Class Members fully performed their obligations under the implied contract with Defendants; however, Defendants did not.

132. As a result of Defendants' breach of these terms, Plaintiff and Class Members have suffered a variety of damages including but not limited to: the lost value of their privacy; not getting the benefit of their bargain with Defendants; the lost difference in the value between the secure services Defendants promised and the insecure services received; the value of the lost time and effort required to mitigate the actual and potential impact of the data breach on their lives.

133. Additionally, Plaintiff and Class Members suffered emotional distress and diminution in the value of their information since their Private Information was unlawfully shared, and likely continues to reside in the possession of, third parties without their consent. Plaintiff and Class Members have been put at an increased risk of future identity theft, fraud, and/or misuse of their Private Information, which may take years to manifest, discover, and detect.

134. Plaintiff and Class Members are therefore entitled to damages.

COUNT V - BREACH OF IMPLIED CONTRACT

(*On Behalf of Plaintiff and the Nationwide Classes, and the State Classes in the Alternative, Against All Defendants*)

(IN ALTERNATIVE TO COUNT IV)

135. Plaintiff re-alleges the preceding paragraphs as if set forth fully in this Count.

136. At all relevant times, Defendants had a duty, or undertook and/or assumed a duty, to implement reasonable data privacy and cybersecurity protocols, including adequate prevention, detection, and notification procedures, in order to safeguard the Private Information of Plaintiff and the Class Members, and to prevent the unauthorized access to and disclosures of this data.

137. Among other things, Plaintiff and Class Members were required to disclose their Private Information to Defendants for the provision of services, as well as implied contracts for

the Defendants to implement data security adequate to safeguard and protect the privacy of Plaintiff's and Class Members' Private Information.

138. When Plaintiff and Class Members provided their Private Information to Defendants in exchange for Defendants' services, they entered into implied contracts with Defendants pursuant to which Defendants agreed to reasonably protect such information.

139. By entering into such implied contracts, Plaintiff and Class Members reasonably believed and expected that Defendants' data security practices complied with relevant laws and regulations and were consistent with industry standards.

140. Under implied contracts, Defendants and/or their affiliated providers promised and were obligated to protect Plaintiff's and Class Members' Private Information. In exchange, Plaintiff and Members of the Class agreed to turn over their Private Information.

141. The implied contracts that include the contractual obligations to maintain the privacy of Plaintiff's and Class Members' Private Information, are also acknowledged, memorialized, and embodied in multiple documents, including (among other documents) Defendants' data breach notification and Defendants' notices of privacy practices.

142. Defendants' express representations, including, but not limited to the express representations found in their notices of privacy practices, memorialize and embody the implied contractual obligations requiring Defendants to implement data security adequate to safeguard and protect the privacy of Plaintiff's and Class Members' Private Information.

143. Plaintiff and Class Members performed their obligations under the contract when they provided their Private Information in consideration for Defendants' goods and/or services.

144. Defendants materially breached their contractual obligations to protect the private information Defendants gathered when the information was accessed and exfiltrated during the Data Breach.

145. Defendants materially breached the terms of the implied contracts, including, but not limited to, the terms stated in the relevant notices of privacy practices. Defendants did not maintain the privacy of Plaintiff's and Class Members' Private Information as evidenced by their notification of the Data Breach to Plaintiff and Class Members.

146. The Data Breach was a reasonably foreseeable consequence of Defendants' actions in breach of these contracts.

147. As a result of Defendants' failure to fulfill the data security protections promised in these contracts, Plaintiff and Class Members did not receive full benefit of the bargain they entered into, and instead received services that were of a diminished value to that described in the contracts. Plaintiff and Class Members, therefore, were damaged in an amount at least equal to the difference in the value between the secure services Defendants promised and the insecure services received.

148. Had Defendants disclosed that their security was inadequate or that they did not adhere to industry-standard security measures, neither Plaintiff, Class Members, nor any reasonable person would have entered into the aforementioned contracts with Defendants.

149. As a direct and proximate result of the Data Breach, Plaintiff and Class Members have been harmed and suffered, and will continue to suffer, actual damages and injuries, including without limitation the release and disclosure of their Private Information, the loss of control of their Private Information, the imminent risk of suffering additional damages in the future, out of pocket expenses, and the loss of the benefit of the bargain they had struck with Defendants.

COUNT VI– UNJUST ENRICHMENT

(*On Behalf of Plaintiff and the Nationwide Classes, and the State Classes in the Alternative, Against All Defendants*)

150. Plaintiff re-alleges the preceding paragraphs as if set forth fully in this Count.

151. Plaintiff and Class Members have an interest, both equitable and legal, in the PII about them that was conferred upon, collected by, and maintained by Defendants and that was ultimately stolen in the Data Breach.

152. Defendants benefitted by the conferral upon them of the PII pertaining to Plaintiff and Class Members and by their ability to retain, use, sell, and profit from that information.

153. But for Defendants' willingness and commitment to maintain privacy and confidentiality, that PII would not have been transferred to and entrusted with them.

154. Because of the Defendants' use of Plaintiff's and Class Members' PII, Defendants obtained an economic benefit over and above what they otherwise would have. Defendants were unjustly enriched by profiting from the additional services and products they were able to market, sell, and create to the detriment of Plaintiff and Class Members.

155. Defendants also benefitted through their unjust conduct by retaining money that they should have used to provide reasonable and adequate data security to protect Plaintiff's and Class Members' PII, as well as profits gained through the use of Plaintiff's and Class Members' PII.

156. It is inequitable for Defendants to retain these benefits.

157. Defendants' retention of wrongfully obtained monies would violate fundamental principles of justice, equity, and good conscience.

158. The benefit conferred upon, received, and enjoyed by Defendants was not conferred officiously or gratuitously, and it would be inequitable, unfair, and unjust for Defendants to retain the benefit.

159. Defendants' defective security and their unfair and deceptive conduct have, among other things, caused Plaintiff and Class Members to unfairly incur substantial time and/or costs to mitigate and monitor the use of their PII and has caused the Plaintiff and Class Members other damages as described herein.

160. Defendants are therefore liable to Plaintiff and Class Members for restitution or disgorgement in the amount of the benefit conferred to them as a result of their wrongful conduct, including specifically: the value to Defendants of the PII that was stolen in the Data Breach; the profits Defendants received and are receiving from the use of that information; the amounts that Defendants overcharged Plaintiff and Class Members for use of Defendants' products and services; and the amounts that Defendants should have spent to provide reasonable and adequate data security to protect Plaintiff's and Class Members' PII.

COUNT VII – DECLARATORY JUDGMENT/INJUNCTIVE RELIEF

(*On Behalf of Plaintiff and the State Classes, Against All Defendants*)

161. Plaintiff re-alleges the preceding paragraphs as if set forth fully in this Count.

162. This Court is authorized to enter a judgment declaring the rights and legal relations of the parties and granting further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal statutes described in this Complaint.

163. An actual controversy has arisen in the wake of the Data Breach regarding Defendants' present and prospective common law and other duties to reasonably safeguard

Plaintiff's and Class Members' PII, and whether Defendants are currently maintaining data security measures adequate to protect Plaintiff and Class Members from future data breaches that compromise their PII.

164. Plaintiff and the Class remain at imminent risk that further compromises of their PII will occur in the future.

165. The Court should also issue prospective injunctive relief requiring Defendants to employ adequate security practices consistent with law and industry standards to protect the relevant PII.

166. Defendants still possess the PII of Plaintiff and the Class.

167. To Plaintiff's knowledge, Defendants have made no changes to their data storage or security practices relating to the PII.

168. To Plaintiff's knowledge, Defendants have made no announcement or notification that they have remedied any and all vulnerabilities and negligent data security practices that led to the Data Breach.

169. Pursuant to its authority, this Court should enter a judgment declaring, among other things, the following:

A. Defendants continue to owe a legal duty to secure consumers' PII and to timely notify consumers of a data breach under the common law, Section 5 of the FTC Act, and various state statutes;

B. Defendants continue to breach this legal duty by failing to employ reasonable measures to secure consumers' PII.

C. Engaging third-party security auditors/penetration testers, as well as internal security personnel, to conduct testing that includes simulated attacks, penetration tests, and audits

on Defendants' systems on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors;

D. Engaging third-party security auditors and internal personnel to run automated security monitoring;

E. Auditing, testing, and training security personnel regarding any new or modified procedures;

F. Purging, deleting, and destroying PII not necessary for provisions of services in a reasonably secure manner;

G. Conducting regular database scans and security checks; and

H. Routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach.

170. The Court also should issue corresponding prospective injunctive relief requiring Defendants to employ adequate security protocols consistent with law and industry standards to protect consumers' PII.

171. If an injunction is not issued, Plaintiff and the Class will suffer irreparable injury and lack an adequate legal remedy in the event of another data breach. The risk of another such breach is real, immediate, and substantial.

172. The hardship to Plaintiff and Class Members if an injunction does not issue exceeds the hardship to Defendants if an injunction is issued. Among other things, if another data breach occurs at one of Defendants, Plaintiff and Class Members will likely continue to be subjected to fraud, identify theft, and other harms described herein. On the other hand, the cost to Defendants

of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendants have pre-existing legal obligations to employ such measures.

173. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach by Defendants, thus eliminating the additional injuries that would result to Plaintiff and Class Members, along with other consumers whose PII would be further compromised.

COUNT VIII - VIOLATION OF THE ILLINOIS CONSUMER FRAUD AND DECEPTIVE BUSINESS PRACTICES ACT, 815 ILCS 505/1, *ET SEQ.*

(*On Behalf of Plaintiff and the State Classes, Against All Defendants*)

174. Plaintiff re-alleges the preceding paragraphs as if set forth fully in this Count.

175. Section 2 of ICFA prohibits unfair or deceptive acts or practices and states, in relevant part, as follows:

> Unfair methods of competition and unfair or deceptive acts or practices, including but not limited to the use or employment of any deception, fraud, false pretense, false promise, misrepresentation or the concealment, suppression or omission of such material fact, or the use or employment of any practice described in section 2 of the "Uniform Deceptive Trade Practices Act", approved August 5, 1965, in the conduct of any trade or commerce are hereby declared unlawful whether any person has in fact been misled, deceived or damaged thereby.

176. Defendants violated Section 2 of ICFA by engaging in unfair acts in the course of conduct involving trade or commerce when dealing with Plaintiff.

177. Specifically, it was an unfair act and practice to represent to the public that they implemented commercially reasonable measures to protect PII, Defendants nonetheless failed to fulfill such representations, including by failing to timely detect the Data Breach.

178. Despite representing to Plaintiff and the State Class members that they would implement commercially reasonable measures to protect their PII, Defendants nonetheless failed to fulfill such representations.

179. Plaintiff and the State Class members have suffered injury in fact and actual damages, as alleged herein, as a result of Defendants' unlawful conduct and violations of the ICFA and analogous state statutes.

180. Defendants' conduct offends public policy as it demonstrates a practice of unfair and deceptive business practices in failing to safeguard consumers' PII.

181. An award of punitive damages is appropriate because Defendants' conduct described above was outrageous, willful and wanton, showed a reckless disregard for the rights of the Plaintiff and consumers, generally, and Plaintiff had no choice but to submit to Defendants' illegal conduct.

COUNT IX - VIOLATION OF THE ILLINOIS UNIFORM DECEPTIVE TRADE PRACTICES ACT, 815 Ill. Comp. Stat. §§ 510/2, *ET SEQ.*

(*On Behalf of Plaintiff and the State Classes, Against All Defendants*)

182. Plaintiff re-alleges the preceding paragraphs as if set forth fully in this Count.

183. Defendants are "person[s]" as defined by 815 Ill. Comp. Stat. §§ 510/1(5).

184. Defendants engaged in deceptive trade practices in the conduct of their businesses, in violation of 815 Ill. Comp. Stat. §§ 510/2(a), including, but not limited to:

A. Representing that goods or services have characteristics that they do not have;

B. Representing that goods or services are of a particular standard, quality, or grade if they are of another;

C. Advertising goods or services with intent not to sell them as advertised; and

D. Engaging in other conduct that creates a likelihood of confusion or misunderstanding.

185. Defendants' deceptive acts and practices include:

A. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's Private Information, which was a direct and proximate cause of the Data Breach;

B. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

C. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's Private Information, which was a direct and proximate cause of the Data Breach;

D. Misrepresenting that they would protect the privacy and confidentiality of Plaintiff's Private Information, including by implementing and maintaining reasonable security measures;

E. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's Private Information;

F. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's Private Information; and

G. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a).

186. Defendants' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of their data security and ability to protect the confidentiality of consumers' Private Information.

187. The above unfair and deceptive practices and acts by Defendants were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff that she could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

188. As a direct and proximate result of Defendants' unfair, unlawful, and deceptive trade practices, Plaintiff has suffered and will continue to suffer injury.

189. Plaintiff and the State Class members seek all monetary and non-monetary relief allowed by law, including injunctive relief and reasonable attorney's fees and costs.

REQUEST FOR RELIEF

WHEREFORE, Plaintiff ask for an award in her favor and against Defendants as follows:

A. Certifying this action as a class action, with the Class as defined above;

B. Designating Plaintiff as representative of the proposed Class and designation of Plaintiff's counsel as Class counsel;

C. For equitable and injunctive relief enjoining Defendants from engaging in the wrongful acts and omissions complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' Private Information, and from failing to issue prompt, complete and accurate disclosures to Plaintiff and Class Members;

D. Awarding compensatory and actual damages to redress the harm caused to Plaintiff and Class Members;

E. Awarding punitive damages as allowable by law;

F. Awarding Plaintiff and the Class Members interest, costs and attorneys' fees;

G. Such other and further relief as this Court deems just and proper.

Dated: June 12, 2024

Respectfully Submitted,

By: /s/ *Kristen A. Johnson*
Kristen A. Johnson (BBO# 667261)
HAGENS BERMAN SOBOL SHAPIRO LLP
1 Faneuil Hall Square, 5th Fl.
Boston, MA 02109
Tel: (617) 482-3700
Fax: (617) 482-3003
kristenj@hbsslaw.com

Plaintiffs' Liaison & Coordinating Counsel

Bryan Paul Thompson
Robert W. Harrer
CHICAGO CONSUMER LAW CENTER, P.C.
650 Warrenville Road, Suite 100
Lisle, IL 60532
Tel. 312-858-3239
Fax 312-610-5646
bryan.thompson@cclc-law.com
rob.harrer@cclc-law.com

Counsel for Plaintiff

E. Michelle Drake
BERGER MONTAGUE, PC
1229 Tyler St., NE, Ste. 205
Minneapolis, MN 55413
Tel: (612) 594-5933
Fax: (612) 584-4470
emdrake@bm.net

Gary F. Lynch
LYNCH CARPENTER, LLP
1133 Penn Ave., 5th Fl.
Pittsburgh, PA 15222
Tel: (412) 322-9243
Fax: (412) 231-0246
Gary@lcllp.com

Douglas J. McNamara
COHEN MILSTEIN SELLERS & TOLL PLLC
1100 New York Ave. NW, 5th Fl.
Washington, DC 20005
Tel: (202) 408-4600
dmcnamara@cohenmilstein.com

Karen H. Riebel
LOCKRIDGE GRINDAL NAUEN PLLP
100 Washington Ave. S., Ste. 2200
Minneapolis, MN 55401
Tel: (612) 339-6900
Fax: (612) 612-339-0981
khriebel@locklaw.com

Charles E. Schaffer
LEVIN SEDRAN & BERMAN LLP
510 Walnut Street, Ste. 500
Philadelphia, PA 19106
Tel: (215) 592-1500
Fax: (215) 592-4663
cshaffer@lfsblaw.com

Plaintiffs' Lead Counsel

CERTIFICATE OF SERVICE

I hereby certify that, on this date, the foregoing document was served by filing it on the Court's CM/ECF system, which will automatically send a notification of such filing to all counsel of record via electronic mail.

Dated: June 12, 2024

/s/ Kristen Johnson
Kristen Johnson